AMENDMENTS TO THE CLAIMS

Please amend the claims on file to read as follows:

Listing of Claims on file

1. [Cancelled] A secure method for generating digital documents that are certified by a known authority, comprising the steps of:

A.   Programming an electronic device with a document issuing method that originates with the known authority, wherein the device further includes means for protecting the programmed method from tampering with;

B.   programming the electronic device with data identifying the owner of the device, and wherein the device includes means to prevent subsequent alterations of the owner identification data;

C.   reading a digital document into the device;

D.   physical identification of the owner of the device, based on the identifying data as programmed in step (B);

E.   if the result of the identification process in step (D) is positive, this indicating that the true owner requested the document, then issuing of a digital document signed by the known authority, wherein the document is prepared according to the document issuing method that was programmed into the device in step A.

2. [Cancelled]   The secure method of claim 1, wherein in step A the programming further includes information that is unique to each device.

3. [Cancelled]   The secure method of claim 1, wherein in step B the device reads a prior issued digital document that attests to a prior identification of the user, and wherein the information in that document is used for programming the electronic device with data identifying the owner of the device.

4. [Cancelled]   The secure method of claim 1, wherein in step C the device reads a digital document relating to the owner of the device, and further including the step of verifying whether the identifying information in the document corresponds to the owner identification data entered in step B; proceeding to step D only if the identification result is positive, otherwise End procedure.

5. [Cancelled]   The secure method of claim 1, wherein in step C the device reads a digital document sent to the owner of the device, and further including the step of

verifying whether the addressee identity information in the document corresponds to the owner identification data entered in step B; proceeding to step D only if the identification result is positive, otherwise End procedure.

6. **[Cancelled]** The secure method of claim 1, wherein in step E the issued digital document is output through a communication channel in the device.

7. **[Cancelled]** The secure method of claim 1, wherein in step E the issued digital document is stored in digital storage means in the device.

8. **[Cancelled]** The secure method of claim 1, wherein in step E the issued digital document is a permit or a certificate.

9. **[Cancelled]** A device for generating digital documents that are certified by a known authority, comprising:

A.   computer means with processing means and memory means for implementing a program written in the memory, and wherein the memory includes a document issuing method that originates with the known authority and data identifying the owner of the device;

B.   means for protecting the document issuing method from tampering with;

C.   means for preventing subsequent alteration of the owner identifing data;

D.   input means for reading information related to physical user identification; and

E.   output means for transmitting digital documents generated in the computer means.

10. **[Cancelled]** The device of claim 9, further including means for storing a plurality of digital documents and for retrieving any document as desired.

11. **[Cancelled]** The device of claim 9, further including an input/output channel for receiving documents or user's commands and for outputting digital documents as desired.

12. **[Cancelled]** The device of claim 9, wherein the device is stored in a wristwatch.

13. **[Cancelled]** The device of claim 9, wherein the device is stored in a smart device.

14. **[Currently Amended]**   A method of ~~authorizing~~ enabling ~~an~~ a user's electronic device ~~to act as a representative of~~ to issue a digital document that is associated with its said user and is certified on behalf of a known certifying authority (CA), comprising:

implementing in the electronic device a document issuing policy of the certifying authority (CA); and

reading into the electronic device a certified digital document associated with ~~a~~the said user; and

generating ~~on behalf of the CA~~ a new ~~certified~~ digital document that is associated with its said user and which is certified by the said electronic device on behalf of the certifying authority (CA) based on the said user's certified digital document and issuing policy.

15. [Previously Amended] The method according to claim 14, wherein information associated with an identity of the electronic device or it's user is stored within the electronic device.

16. [Currently Amended] The method of claim 14, wherein the issuing policy attests to personal identifying information of the ~~device~~ user of the device.

17. [Previously Amended] The method of claim 14, wherein the new certified digital document is output by the electronic device through a communication channel.

18. [Previously Amended] The method of claim 14, wherein the certified digital documents are permits or certificates.

19. [Currently Amended] The method of claim 14, wherein a person using the electronic device to sign or certify a digital document is requested to identify ~~themselves~~ himself prior to the electronic device signing or certifying the digital document.

20. [Currently Amended] The method of claim 19, wherein a user identifies ~~themselves~~ himself using biometric identification information.

21. [**Previously Amended**] The method of claim 14, wherein a plurality of certified digital documents associated with the user are stored within the electronic device, each of which plurality of certified digital documents is associated with a different certifying authority.

22. [**Currently Amended**] An electronic device <u>associated with a user</u> adapted to act as a representative of a certifying authority <u>(CA)</u> comprising:
a controller adapted to execute a program associated with the certifying authority <u>(CA)</u> based on a document issuing policy of the certifying authority <u>(CA)</u>, reads a certified digital document associated with a<u>its</u> user, and based on the <u>user's</u> certified digital document generates a new digital document <u>associated with the said user and certified on behalf of the said certifying authority (CA)</u> in accordance with the document issuing policy.

23. [**Currently Amended**] The electronic device according to claim 22, wherein the program generates the new certified digital document from a certified document associated with a <u>the</u> user if data in the certified document is consistent with the document issuing policy.

24. [**Previously Amended**] The electronic device of claim 22, wherein the controller reads a digital document provided to the electronic device and signs or certifies the digital document only after the electronic device attests to personal identifying of the user.

25. [**Previously Amended**] The electronic device of claim 24, further comprising a biometric data input module.

26. [**Previously Amended**] The electronic device of claim 22, wherein a plurality of certified documents associated with the user are stored within the electronic device, each of the plurality of certified documents are associated with a different certifying authority.

27. **[Previously Amended]** The electronic device of claim 22, wherein the electronic device is functionally associated with a wristwatch.

28. **[Previously Amended]** The electronic device of claim 22, wherein the electronic device is functionally associated with a smart card.